global
conference
partners TM

Via Electronic Delivery

Ms. Marlene H. Dortch
Federal Communications Commission
The Portals, TW-A325
445 12th Street SW
Washington, DC 20554

Re: EB Dkt. No. 06-36
Global Conference Partners' 2008 Privacy Procedures

Dear Ms. Dortch:

I, Clifford Kaylin, certify that I am the Chief Technology Officer of Global Conference Partners (GCP) and, acting as an agent of GCP, that I have personal knowledge of the operating policies and procedures to protect the subscriber information of GCP's services.

GCP is an end user of telecommunications services and a provider of information services, 47 U.S.C. § 153(20), and is not a telecommunications carrier subject to the FCC's CPNI regulations, 47 C. F. R. § 64.2001 *et seq.* GCP is aware of the FCC's June 30, 2008 *InterCall Order* (FCC 08-160) finding that InterCall's audio bridging service may be "telecommunications" under the federal Communications Act. GCP (and others) filed a petition for reconsideration of the *InterCall Order* on July 30, 2008, and reconsideration is currently pending before the Commission. In any event, the *InterCall Order* appears limited to the federal Universal Service Fund obligation and so did not apply CPNI or other telecommunications regulations to providers of InterCall-like audio bridging services. *Id.*, at n. 49 (Intercall Order "pertains solely to universal service contribution obligations"). As such, GCP is not required to make an annual CPNI certification filing.

In any event, GCP files the attached statement regarding its 2008 subscriber privacy policies out of an abundance of caution and in order to minimize the unnecessary expenditure of resources for the FCC and itself.

GCP has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. GCP has not received any customer complaints in the past year concerning the unauthorized release of subscriber information.

global
conference
partners TM

Further, I certify that the attached Statement of GCP's Subscriber Privacy Policies accurately reflects the policies that are in place, as a good business practice, in order to protect the privacy of GCP's subscriber information.

Signed _____

Clifford Kaylin

Chief Technical Officer

425 E. Colorado Street, Suite 500, Glendale, CA 91205 USA
+1 818.553.1800 | +1 818.553.1427 (fax)
www.globalconferencepartners.com

Accompanying Statement Regarding GCP's Subscriber Privacy Policies for 2008

Global Conference Partners is a conference call service provider and is not a telecommunications carrier. We connect our equipment as customer premises equipment and have only limited access to CPNI in the form of call detail records.

If a caller into GCP's service uses a non-toll-free number to access our conference equipment, we do not to provide the calling party's information to anyone under any circumstances. If the caller to the GCP service uses a toll-free number, GCP will provide the calling party information to the conference organizer, as permitted by tariff.

GCP secures its databases under multiple layers of security – physically, our servers are placed behind multiple locked enclosures and doors. The data cannot be accessed remotely except by senior operations personnel and only after authenticating. GCP has implemented network security measures to protect customer account information including, but not limited to, the use of encryption.

GCP has implemented password protection for online accounts and has procedures in place for lost or stolen passwords.

GCP employs a third-party data security validation service (Trustwave) who conducts monthly "penetration tests" to validate that our network and data infrastructure meets all current PCI compliance standards. GCP ensures that it passes these tests.

To the extent that we communicate with our customers, we respect all opt-in preferences established by the customer. The customer is asked to choose whether to opt-in at the time they sign up for the service with GCP. Customers must authenticate their identity when changing their opt-in preferences or other personal data on our web site.

GCP will notify law enforcement within seven days of the reasonable discovery of a data breach involving CPNI. GCP will also notify affected customers as permitted to do so by law. GCP will maintain a record of such notifications.

GCP tracks customer complaints it receives regarding CPNI.

GCP currently does not use CPNI to market outside of the category of service to which the customer subscribes. If GCP subsequently determines that it wants to use CPNI for marketing purposes, then it will provide the appropriate customer notification. GCP maintains a list of customers who have opted out from receiving marketing communications with the company and will respect those customer preferences at all times in the future. GCP does not share CPNI with joint venture partners or independent contractors for marketing purposes.